SecureAware®

Super User Manual

Applies to SecureAware version 3

Document date: June 2009

About this document

This manual guides a Super User through the key functions required for setting up, configuring and managing the SecureAware system. Functions covered include:

- Access restriction
- Document management
- Report configuration

neupart
Information Security Management & Awareness

Table of content

My SecureAware – the start page

When you log on to SecureAware for the first time, you will most likely see the screen below. This is the start page, referred to as My SecureAware which, unless you change the settings (see the chapter *"What should my users see when they log on?"*) will be the start page for all your users. My SecureAware consists of four different parts (tabs).
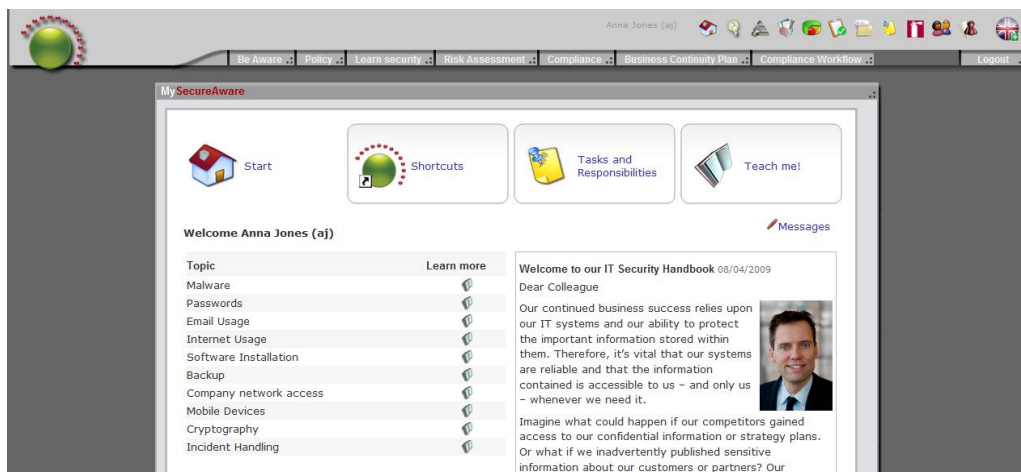

The **Start** tab

The first tab – Start – shows shortcuts to education content. As soon as you start creating a policy set, risk assessment, awareness quiz or compliance evaluations, the results/status of these will be shown here as in the screen below.
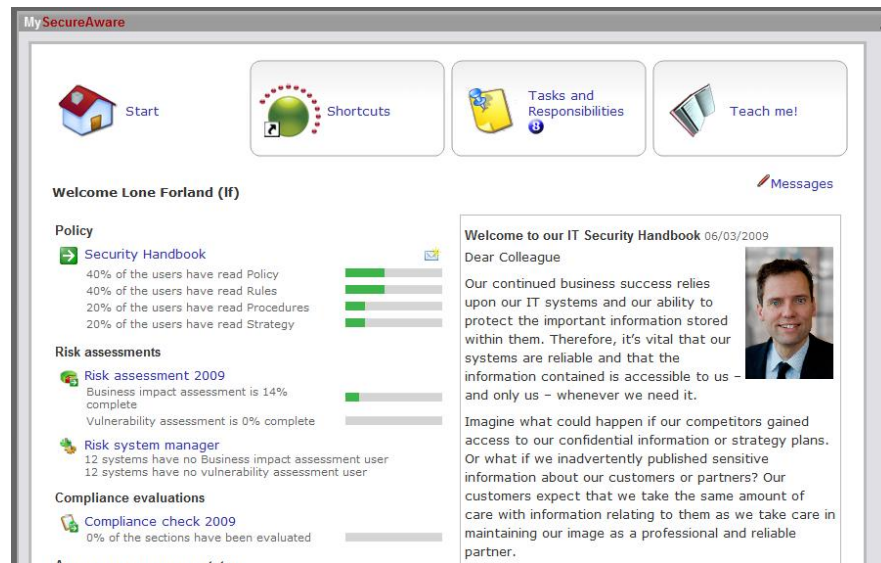
The bulletin board on the right hand side is where you can display messages to your users. To create a new message (or delete the default one), click on **Messages**. Now select either the message you would like to edit or **Write message** to create a new message on the bulletin board.
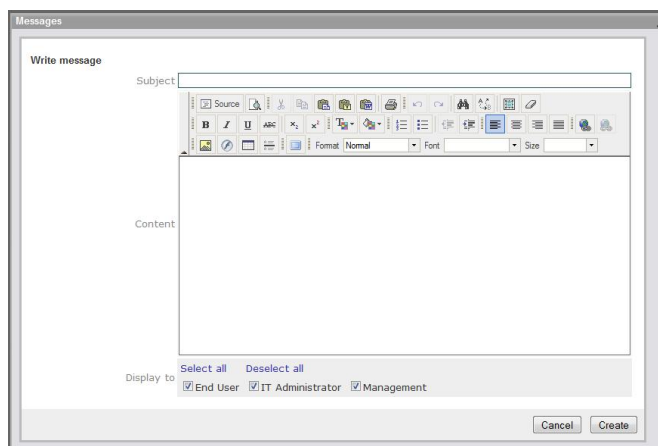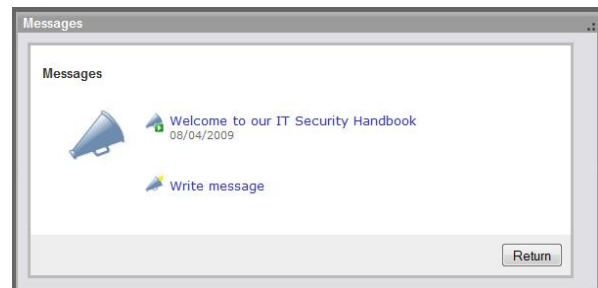
When creating a new message, remember to select which target groups it should be shown to. After clicking **Create** you will see an e-mail icon in the bottom of the screen. Click on it to write a notification about this to your users.

The **Shortcuts** tab
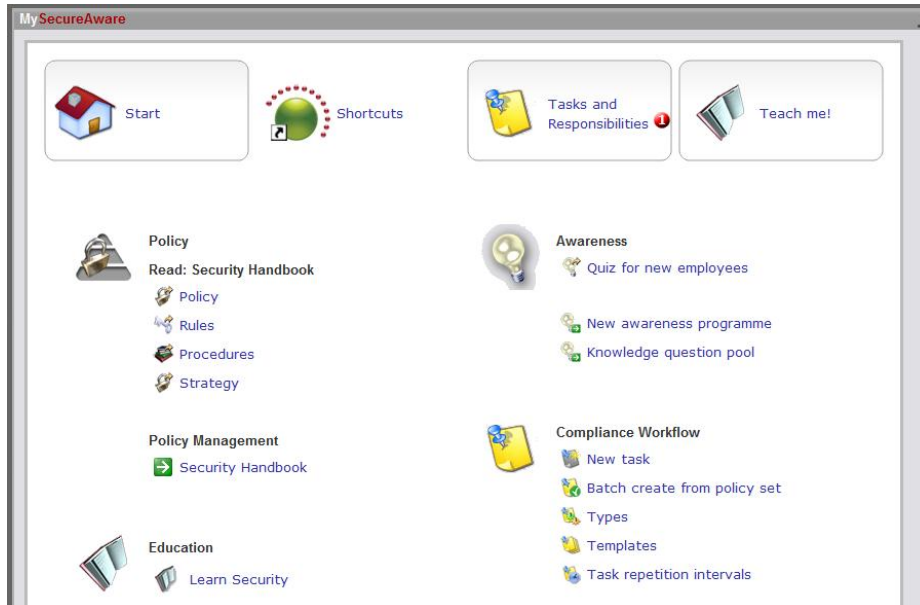
The tab Shortcuts gives you – as the name implies - a range of shortcuts to different functions in SecureAware.

The tab **Tasks and Responsibilities**

The Tasks and Responsibilities tab gives you an overview of the tasks you have to carry out in SecureAware (left hand side). Click on the task to go directly to carrying it out. On the right hand side all your responsibilities are listed i.e. systems, assets or procedures. You can click on any of these (given you have the access rights necessary) to access it directly.
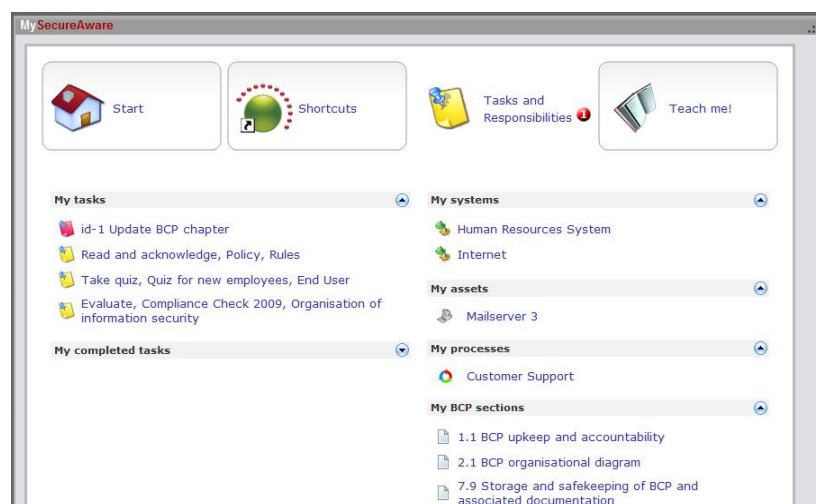
The **Teach Me!** tab
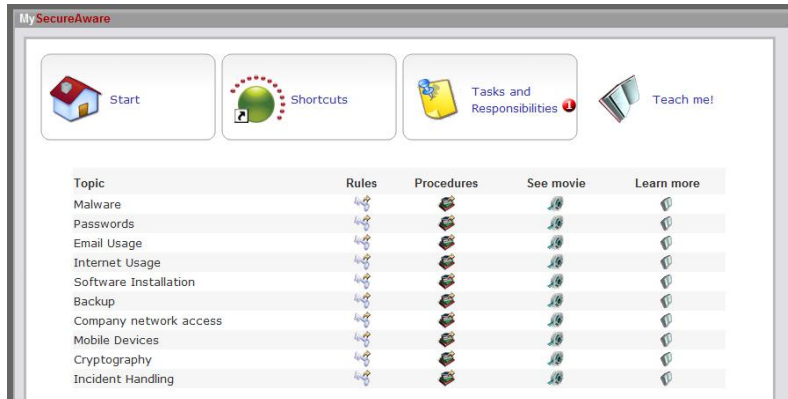
Under the Teach Me! Tab you – and your users – have easy access to education content of various forms. You have direct links to the rules and procedures of your policy set divided into topics of your choice. If you use the default SecureAware topics, your users will have access to education content and films covering these topics.
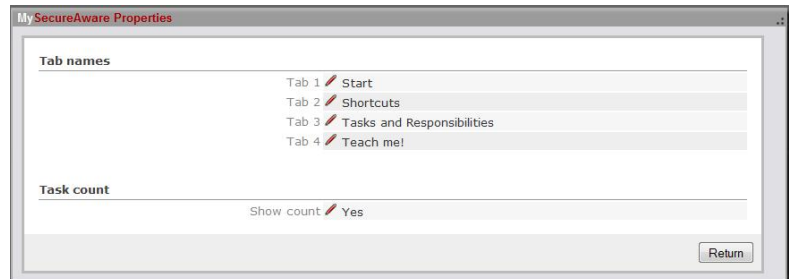
What should my users see when they log on?

If you would rather have your users see another page when they access SecureAware, this is easily changed. Click on the Configuration icon in the top right corner of the screen and then click on **Properties** just below **Start Page**.
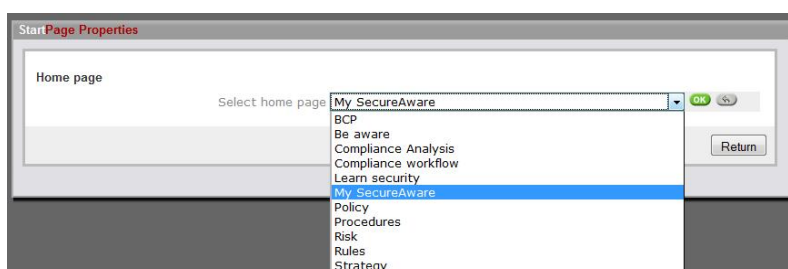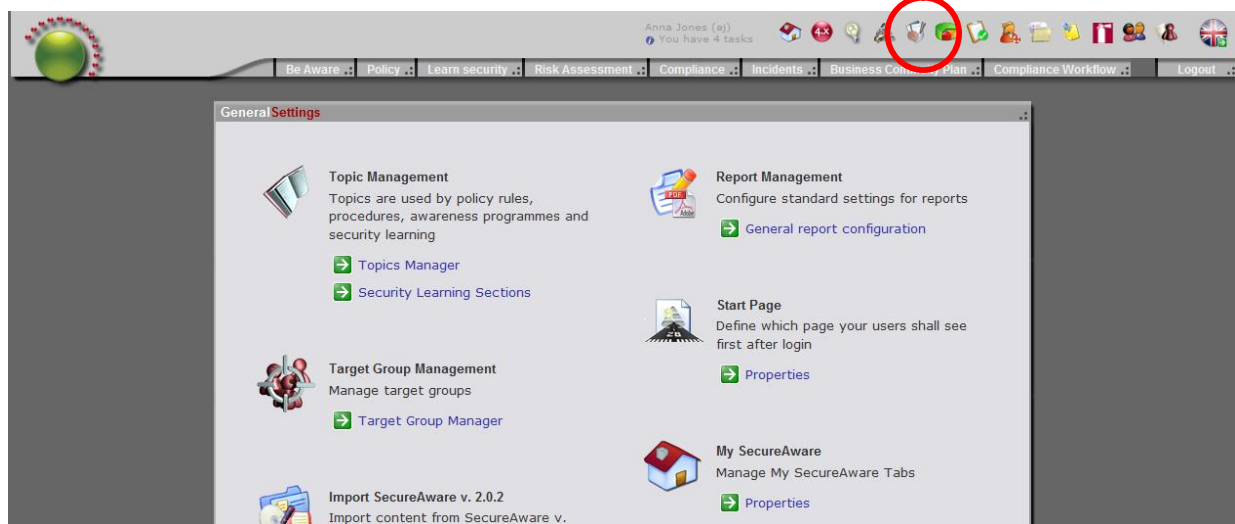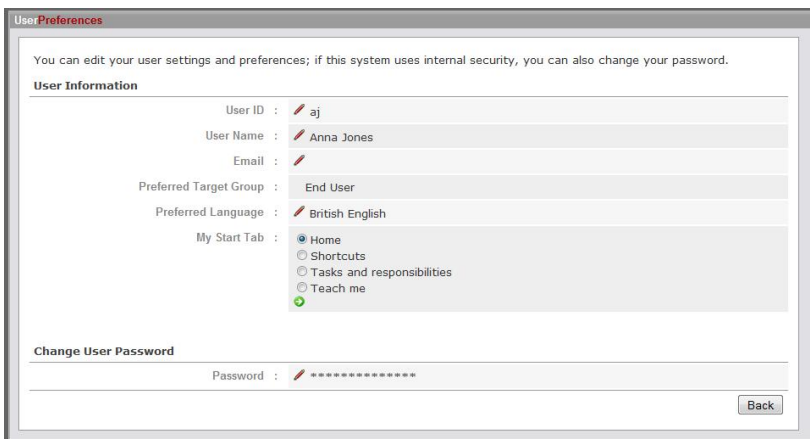

Now click on the pencil and use the drop down box to select the start page of SecureAware. Remember to click OK before you click return.

If you want to change the name of the tabs on My SecureAware, click on **Properties** under **Manage My SecureAware Tabs**. Now click on the pencil in front of the tab you want to change the name of, write the new name and click OK.

Your users will be able to select themselves which tab to see as the first on My SecureAware. To do this, the user must click on the **User Preferences** icon in the top right corner, click on the pencil for **My Start Tab,** select the tab and click the arrow button to save the

changes.

User Configuration

Once you have logged on as a Super User (SU), you can configure a wide range of settings relating to your SecureAware users. If you have yet to change your password, use the default password: **snRt!32w**

When successfully logged on, you will be able to see the Super User menu bar at the top right of your screen (shown below). The number of icons shown can vary according to the number of modules your company is licensed to use. To access the User Management module click on the icon.
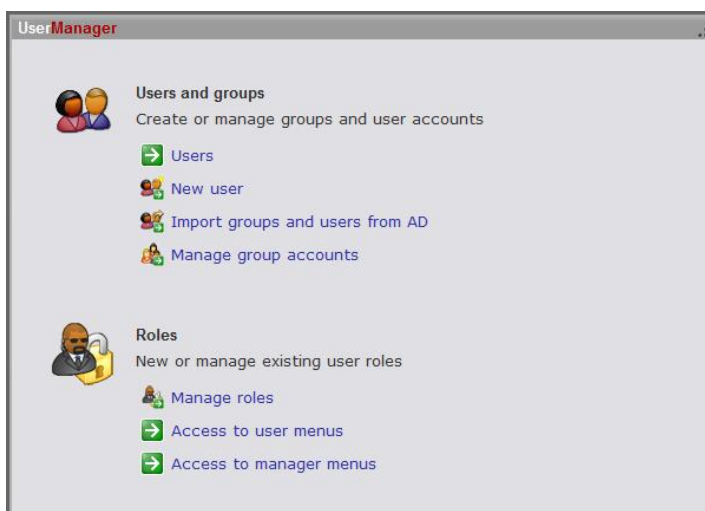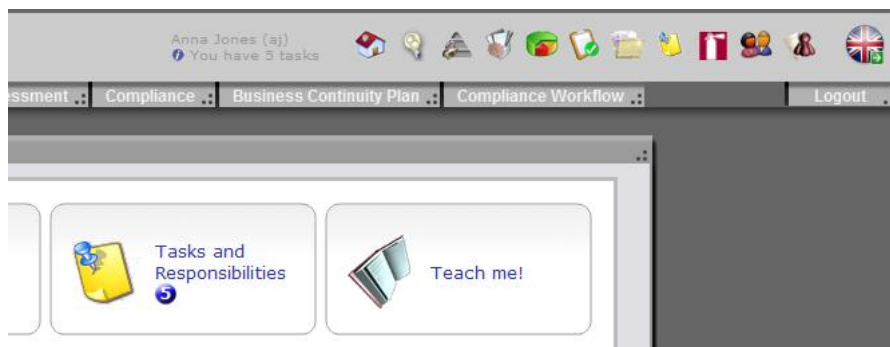
You now have access to the main User Management menu.

User Roles

Different users require access to different SecureAware functions. Assigning individual access rights and tasks on a user-by-user basis can be time consuming, but with SecureAware's 'role' system you can do this quickly and easily.

Role management

SecureAware comes with a selection of standard pre-defined user roles, each of which in turn holds a number of associated access rights. Click on ➡ **Manage roles** to view, edit and create new roles.
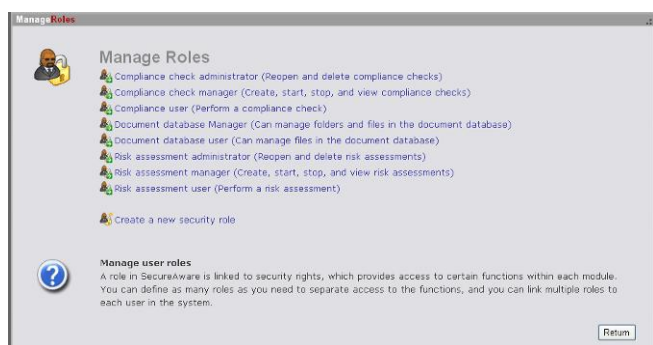
You will now see the standard roles that already exist, as well as the functions to which each different role has access. By clicking on a specific role you can edit the role's name and description, and add or remove access rights. Click on the ✏ icon to edit or the ✗ icon to delete. If you want to give new access rights to a role, click 🖼 **Add** and select from the drop-down menu. Remember to click on 🆗 once you have made your changes.

If you want to create a new role, click on 👤 **Create a new security role,** enter a name and description (if required) then click **Create.** The new security role will now be featured on the list of roles in the **Manage Roles** menu and can be edited in the same was as for the others (as described above).

Access roles

Once you have revised and tailored the listed roles, you can start restricting or granting certain roles access to the various SecureAware end-user menus and program management functions. To do this,

select and edit the roles which you wish to have access to or be barred from any desired function. If a user is a member of one or more of these role groups, he or she will automatically be given or denied access.

Menu Access Roles

The end-user menu is shown as a selection of tabs at the top of the screen.

You can determine which roles are able to view the different end-user menu tabs by clicking on ➡ **Menu Access roles**. Select a role by clicking on 🌟 **Add** next to the appropriate module name and select from the drop-down menu. Click **OK** to add. You can add as many roles as you like and delete them at any time by clicking on ✗.

In addition to SecureAware's predefined roles and those created by a Super User, there are three standard roles for the end-user menu which can not be changed. These are:

- 🔴 **Anonymous users** – any user not logged on to SecureAware. (The standard program setting allows these users to view the Learn Security section only, but this can be extended.)
- 🔴 **Validated users** – all users who are logged on to SecureAware, either directly or through the AD.
- 🔴 **All users** – as the name suggests, all users whether logged on or not.

Management Roles

Access to the system management menu can be limited in the same was as for the end-user menu. The SecureAware management section is the section accessible using the module icons in the top right-hand corner of the screen.
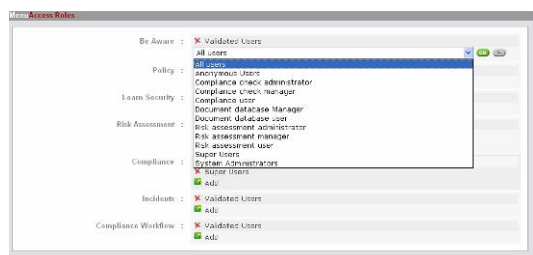
Note: standard setup allows validated users access to My User Preferences and language selection only. The role of Super User can not be removed from the list of roles with access to the management section as this would cause a lock-out situation in which no one would have access to the SecureAware management functions.

It is important to remember that even if a user has access to this section of SecureAware, in order to carry out tasks (for example, to run a compliance check), he or she must be granted specific access to the individual management function.

User setup and management

Creating a new user

To manually create a new SecureAware user click on **Create new user account**. You can now enter a user ID of your choice (to be used as a log in) and the user's name. Now click **Create.**

Now you can enter the users email address (optional). You can also state which language should be used as standard for this new user, though this can be altered by the user at a later date. The language settings and password can be changed by the user and it is highly advisable that you encourage the user to create his or her own personal password after logging on for the first time.

Assign a user to a specific target group and allocate the user roles by clicking on the blue crosses and selecting from the list.

By adding a user to specific target group you can, for example, configure the way in which the user is presented with security policy rules. Users themselves are able to change the user group in which they are included so listing users in target group is, in itself, not a form of access limitation. Note: a user may belong to more than one group at a time.

By allocating roles to a user, the user will be granted access to all those functions which are linked to that specific role. The allocation of functions to the various different roles is managed from the main SecureAware User Manager menu as described in the next chapter.

Managing your user accounts

In the main User Manager menu, click on

➡ **Manage user accounts**. You will now be shown a complete index of all existing SecureAware users. If you have many users you can use the letters at the top of the menu to view them listed alphabetically. You can also search for a specific user using by entering all or part of a name in the blank search box and clicking 🟢. A user's details may be edited at any time by clicking on the 🖊 next to his or her name. The menu here also allows you to add new users or import external users (see below).

Importing external users

If the import of users via LDAP has been authorized by your system administrator, this can be done by clicking on ➡ **Import external users** followed by entering your administrator username and administrator password (for LDAP).

Importing groups from an AD
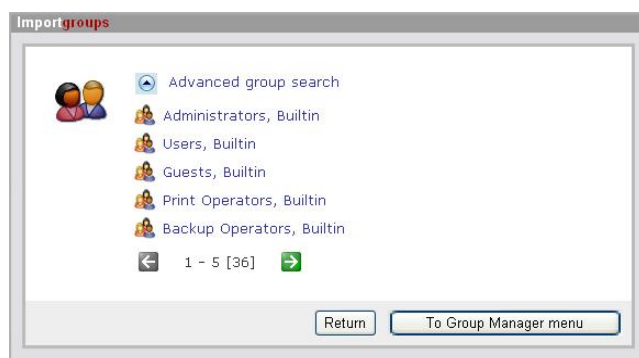
If you wish to import groups, select the **Import groups and users from AD** option in the main User Manager menu. Once logged in, you can view a list of all the groups in the company AD. Use the green arrows to move backwards and forwards through the list of groups. Click on the desired group to import.

To search for a specific group used the 🔵 Advanced group search function. You can use this advanced search to carry out a search with specific search criteria. For example:

(&(&(objectCategory=person)(objectClass=group))(&(memberOf=CN=Group Name,OU=Name,DC=server,DC=server)))

When you have imported a group, it will be removed from the list here. By now clicking on the **Group manager** button (at the bottom right of the window) you will now be able to configure various elements of the selected groups, such as adding to target groups and allocating specific roles.

Configuring your groups

To change the configuration and set up of a group, simply click on the group name. To delete a group from SecureAware click on ✗. If the group has yet to be imported from an AD, select **Import group from AD**.

Although it is, in effect, possible to create a new group directly within SecureAware this practice is not advisable. Instead, it is recommended that any new groups be created in an AD then subsequently imported from the AD into SecureAware.

Once imported, groups can be listed under specific target groups and allocated roles by selecting ✦.

In the same way as for users, by listing a group under a specific target group you can configure the way in which its users are presented with security policy rules. Users themselves are able to change the user group in which they are included so listing under a target group is, in itself, not a form of access limitation. Note: a user may belong to more than one group at a time.

By allocating roles to a group, the group users will be granted access to all those functions which are linked to that specific role. The allocation of functions to the various different roles is managed from the main SecureAware User Manager menu as described in the next chapter.

Altering a group name or key is NOT recommended. This should only be done when absolutely necessary.

Restricting access to the Policy module

A user's access to the contents of the Policy module's rules and procedures can be restricted as required. This can be done by either linking roles directly to individual rules (or more specifically, objects) and procedures, or by linking rules to already existing SecureAware groups.

Group-based access restriction

Most of the rules (objects) and procedures in SecureAware are

already linked to specific user groups (Target groups) and group-based access restriction is easily established. To set up a group-based access restriction click on the ⬡ Configuration Management icon at the top right of the screen then select ➔ **Target Group Manager**.

SecureAware has three standard user groups – End User, IT Administrator, and Management – but you can create and add as many new groups as you require by selecting the 🧑‍🦰 **Create new target group** function. Once you have given your new group a name, it can be edited in the same way as the existing groups.
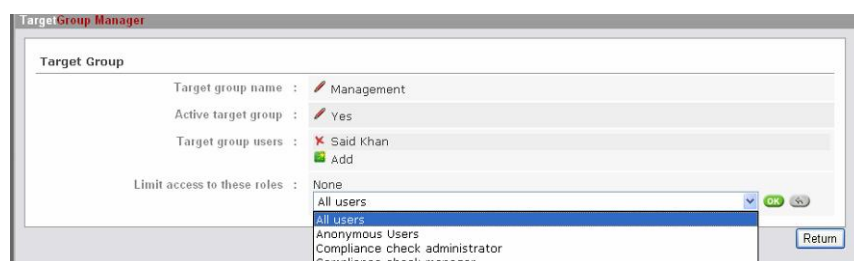
You can add users to a group by selecting the desired group, clicking 🧑 **Add**, and searching for the user you wish to add. You may instead choose to add a block group of users who share the same role. By granting access to a specific role, any user who shares that role will be able to view the rules and procedures applicable to the target group.

In the following section it important to remember that if access to rules and procedures is not limited to one or more target group, these rules and procedures will be viewable by everyone.

Access to rules and procedures

To limit user access to the Policy manual's rules, click on the ⛰ Policy Management module icon at the top right of the screen and then open the ⊙**Show advanced management** menu on the left. Click on 🏛 **Security objects** and then select the required security object from the left-hand menu. You can now decide who you want to have acces to that specific object and its associated rules.

The Access rights tab

Use the **Access rights** tab if you want to restrict certain roles from viewing the selected security object. Remember to click on OK after each selection.

The Target Group tab

Alternatively, you can link a target group to the selected security object by using the **Target Group** tab. Remember to click on ➡ after each selection.

If you choose to limit access to certain rules, you should be aware that your access restrictions will be effective in all of the SecureAware modules in which those rules appear – including in the Awareness program policy tests.

To limit access to procedures, open the Policy Management module ⛰ and click on the required policy name on the top left of the menu. In the same way as for the rules, you can now choose which user groups and/or roles have access to view that particular procedure.

Document Manager

Using SecureAware's Document Manager module, you can upload and index the documents relevant for maintaining you company's IT security standards and you can specify which roles you want to have access to read, edit or delete files. Open the Document Manager by clicking on the icon at the top right of your screen.
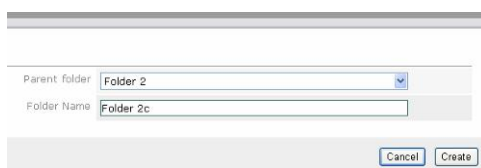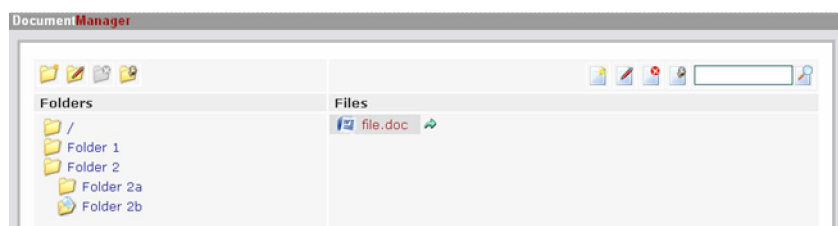
Create a new folder by clicking on the icon. Give the folder a name and (if necessary) select a Parent folder in which to place your new folder.

You can edit a folder by clicking on or delete using . You can configure a folder's security settings using the icon. In the example shown, Super Users have access rights to read , create , edit , and delete folders. Super Users are also able to create and delete files within this folder. SecureAware's standard settings are fixed to ensure unlimited editing access to any Super User. In the example, validated users only have access to read the contents of the folder. Status can be changed by clicking / . To add new folder roles, select them from the drop-down menu and to delete existing roles click on .

17
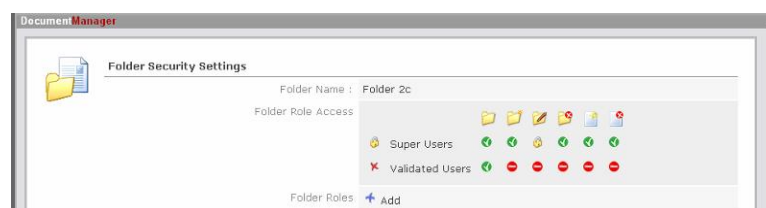
To upload files, click on then locate the required file from the library. Clicking on **Create** will upload the file to the open folder. Once uploaded, the file can be edited or deleted . As for access to folders, access to files can be limited. To restrict file access, select the file and click on the File Security icon .

Report Configuration

The layout and look of SecureAware's reports can easily be tailored to fit your specific company and needs. Click on the Configuration Management icon at the top right of your screen then select ➔ **General report Configuration**.

Now you can edit the print size of your report and margin color (optional) using the editing pencil icon. You can also choose to include a table of content or upload a report background. Remember to click on **OK** once you have made your changes.

Requirement Management

SecureAware comes with a number of standards. The chapters in the standards are mapped to the rules in the rule library. You can choose to add mapped rules to the standard or to create your own "standards". To do this, go to **Configuration > Requirement Set Manager.**
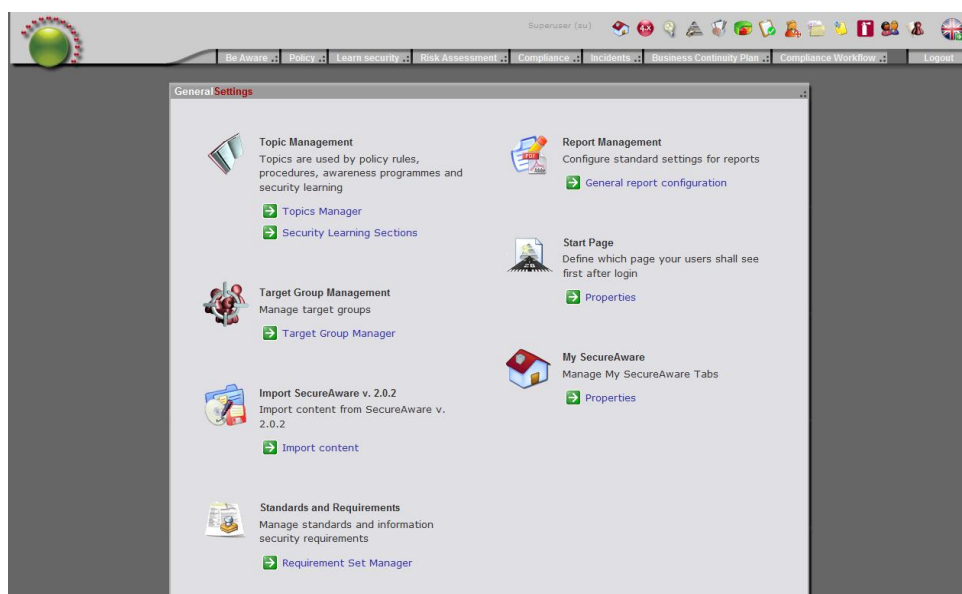
Create/edit standard

Click New requirement set and type the name of the standard/requirement set and click Create. The standard will now appear in the list of standards. **Click on the name > Chapter Manager** to start creating chapters. Type a name, title and a description and select where the chapter should be
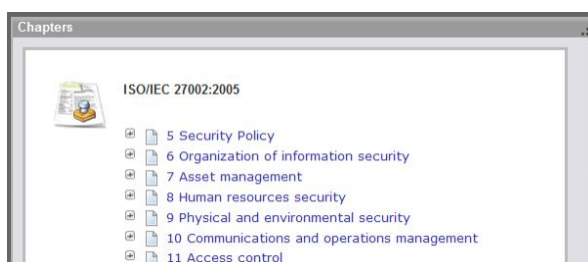

placed. This is done by selecting the parent chapter in **Select Chapter**, and the chapter which it should succeed in **Place after chapter.** Example: Chapter 3.4.2's parent chapter is 3.4 and it should be placed after chapter 3.4.1.

Mapping standard chapters to rules

You can map the standard chapters to rules in the rule library in two ways: If you know which rule you want to map to, click **Add**, type (a part of) the name of the rule and click the green arrow. You can also use the Smart match search which uses the content of the chapter title to search for rules which could match the chapter.
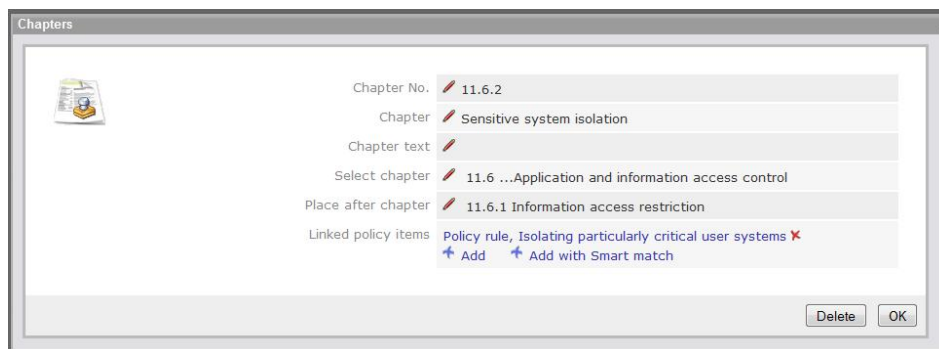
You map a rule by clicking on it. Mapping to a rule indicates that no matter which of the rule's options are selected in the it security handbook, the requirement is complied with. If you want to indicate that a certain option must be chosen in order to comply with this requirement, fold out the rule (+) and select the necessary options by clicking on them.
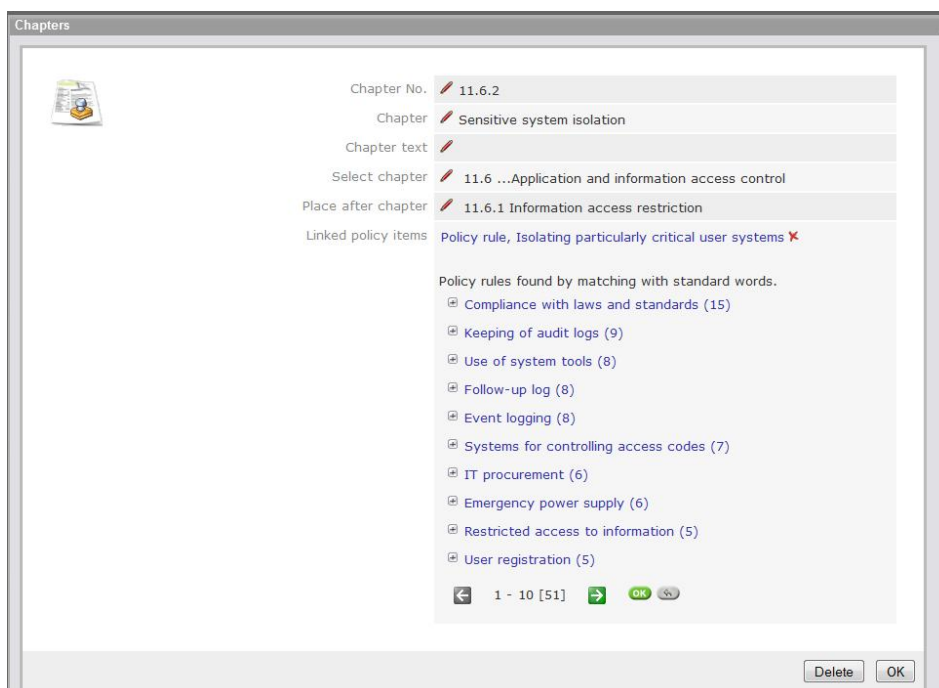
Contact Information

- Further information is available by contacting Neupart

Europe

Neupart A/S

Hollandsvej 12

2800 Lyngby

Denmark

Tel +45 7025 8030

Fax +45 7025 8031

Neupart GmbH

Kaiserwerther Strasse 115

40880 Ratingen/Düsseldorf

Germany:

Tel. +49 (0) 2102/4209-26

Fax +49 (0) 2102/42062

North America

United States

Neupart Inc.

2553 Crescent St

Ferndale, WA 98248

Tel. 360-820-2545

Fax 360-392-6078